

AMENDMENTS TO THE CLAIMS

Claims 1-34 (canceled)

Claim 35 (new): A method of recording digital data onto a medium using only a digital watermark to control a recording process and for indicating the addition of a copy mark to the digital data, comprising the steps of:

- (a) detecting from said digital data any digital watermark that may be electronically embedded in said digital data, wherein said digital watermark is electronically embedded in said digital data through a transformation of said digital data;
- (b) if said digital watermark is detected, determining if said digital watermark specifies that a copy mark be embedded in said digital data so as to control subsequent recording of said digital data;
- (c) if the results of said detection and said determination indicate that subsequent recording of said digital data is to be controlled, embedding a copy mark in said digital data;
- (d) scrambling said digital data together with said watermark and said copy mark using an encryption key;
- (e) encoding said scrambled digital data using said encryption key; and
- (f) recording said scrambled and encoded digital data onto a medium so as to control subsequent copying or playback of said digital data as a function of said copy mark.

Claim 36 (new): The method of claim 35 wherein said copy mark indicates whether copying/recording of said digital data is to be stopped or continued.

Claim 37 (new): A method of performing playback control of digital data that is both scrambled and encoded using a common encryption key for both scrambling and encoding, to thereby produce scrambled and encoded digital data, wherein said scrambled and encoded digital data is then recorded onto a medium, comprising the steps of:

- (a) reading said scrambled and encoded digital data from said medium to thereby produce read digital data;
- (b) descrambling and decoding said read digital data using said common encryption key, to thereby generate descrambled and decoded digital data;
- (c) detecting any digital watermark and copy mark that is electronically embedded in said descrambled and decoded digital data, wherein said digital watermark is embedded in said descrambled and decoded digital data through a transformation of said digital data, and wherein said copy mark is embedded in said descrambled and decoded digital data as a function of a content of said digital watermark; and
- (d) controlling playback of said descrambled and decoded digital data using only said copy mark.

Claim 38 (new): A video driver card for decoding scrambled and encoded digital data wherein original digital data is both scrambled and encoded using a common encryption key, comprising:

- (a) means for both descrambling and decoding said scrambled and encoded digital data using said common encryption key, to thereby reproduce said original digital data;

- (b) means for detecting from said original digital data any digital watermark and digital copy mark electronically embedded in said original digital data, wherein said electronically embedded digital watermark is embedded in said original digital data through a transformation of said original digital data, and wherein said embedded digital copy mark is embedded in said original digital data as a function of a content of said digital watermark; and
- (c) means for controlling inhibition of playback of said original digital data using only digital copy mark.

Claim 39 (new): The video driver card of claim 38 wherein said original digital data is an MPEG stream, and wherein said means for controlling inhibition of playback (c) includes means for determining whether or not outputting said MPEG stream is to be performed, and includes means for outputting said MPEG stream.

Claim 40 (new): A player for playing-back scrambled and encoded digital data that is recorded onto a medium, wherein both scrambling and encoding of said digital data is performed using a common encryption key, comprising:

- (a) means for reading said scrambled and encoded digital data from said medium;
- (b) means for both descrambling and decoding said read digital data using said common encryption key, to thereby recover said digital data;
- (c) means for detecting from said recovered digital data any digital watermark and digital copy mark that is electronically embedded in said recovered digital data, wherein said digital watermark is electronically embedded through a transformation of said digital data, and wherein

said digital watermark is electronically embedded as a function of a content of said digital watermark; and

(d) means for controlling inhibition of playback of said recovered digital data using only said detected copy mark.

Claim 41 (new): The player of claim 40 wherein said recovered digital data is an MPEG stream, and wherein said means for controlling inhibition of playback (d) includes means for determining whether or not outputting of said MPEG stream is to be performed, and includes means for outputting said MPEG stream.